安全协议

2020年8月25日 13:16

1. IPSec：IETF指定IPv6过程中处于security考虑制订的协议
    a. 基本概念
        i. Security Association 安全关联 SA：保护通信的单向逻辑连接
        ii. 隧道：把包封装在新包中，新包的IP头目的地址通常是IPSec防火墙
        iii. Internet安全关联和密钥管理协议 ISAKMP：定义了密钥管理表述语言通用规则及要求，为安全关联和密钥创建了标准通用框架
        iv. Domain of Interpretation 解释域 DOI：IANA的命名空间，为ISAKMP统一分配标识符
    b. 组成
        i. Authentication Header 验证报头 AH协议
            1) 能为IP通信提供数据源认证、数据完整性、抗重放保证，但不能防止窃听，因此适合传输非机密数据
            2) （IP头后的）扩展报头结构（需参与认证）
                a) 8位下一个报头的协议类型
                b) 8位AH头载荷长度，由于IPv6的扩展头相关规定，此值需-2（单位32位）
                c) 16位保留数据，暂时全0
                d) 32位安全参数索引，为识别SA的位随机值，0表示无SA，1~255被IANA保留
                e) 32位序列号，可抗重放
                f) 可变长认证数据，默认96位，必须是32位的倍数，包含了数据包完整性校验值ICV，一般是消息认证码MAC，计算时忽略IP报头的TTL和服务类型等可变字段
        ii. Encapsulating Security Payload 封装安全有效载荷 ESP协议
            1) 提供机密性保护、有限的流机密性保护、无连接的完整性保护、数据源认证和抗重放攻击等安全服务
            2) 和AH一样，通过进入和外出的处理还可提供访问控制服务
            3) 和AH的主要优势是机密性保护、有限的流机密性保护
            4) 加密服务是可选的，启用后可获得完整性和认证
            5) 一般不加密IP头只加密有效载荷，在端对端隧道通信时全加密
            6) （IP头后的）扩展头格式（需参与认证）
                a) 32位安全参数索引，和IP头目的地址、ESP协议一起标识SA
                b) 32位序列号
                c) 变长的载荷数据，包含下一个头字段所指示的数据
            7) （IP载荷数据后的）尾部格式
                a) 变长填充项，可用于隐藏载荷实际长度

b) 8位填充项长度，单位字节
c) 8位下一个头，标明下一个IP协议号的报头
8) 变长认证数据ICV：紧跟于尾部，对前几项计算所得，一般不加密

iii. Internet Key Exchange 互联网密钥交换 IKE 协议
1) 主要负责IPSec的密钥管理，尤其是当用户数较多时由IKE动态维护
2) 基础是ISAKMP的基础、Oakley的模式和SKEME的共享和密钥更新技术
3) 阶段一建立IKE SA，阶段二用阶段的SA协商并建立其他SA
4) 定义的交换模式：主模式、野蛮模式、快速模式、新群模式
5) 允许的认证方法：数字签名、公钥加密、基于修订的公钥加密、基于预共享密钥的认证

c. 工作模式
i. 传输模式：保护IP载荷，不改变IP头，只适用于端到端安全通信
ii. 隧道模式：保护整个IP包，新加一个IP头，此时AH或ESP扩展头出现在两个IP头之间

d. 应用：作为IPv6的组成部分，基本可以和各种网络协调工作

2. Secure Sockets Layer 安全套接字层 SSL：Netscape于1994提出的传输层上应用层下的加密及身份认证通信协议，后被IETF采纳，制订了TLS标准
a. 提供的服务
i. 客户机和服务器的合法性认证
ii. 加密数据以隐藏被传送的数据
iii. 数据完整性

b. 工作流程：接通、密码交换、会话密码、检验密码、客户认证、结束
c. 结构：
i. 握手协议：互相认证、交换密钥、创建会话、在会话中建立多个临时连接
ii. 记录协议：分片、压缩、尾部添加消息认证码、整体加密、头部添加SSL记录协议头（包括8位标明协议，8位标明SSL主要版本号，8位次要版本号，16位标明压缩后数据长度）等工作提供机密性和消息完整性

d. HTTPS：HTTP加上TLS或其前身SSL
i. 设计目标：数据保密性、数据完整性、身份校验安全性
ii. 双向身份认证：基于X.509证书。客户端发起SSL握手请求，服务端发送证书、客户端检查，客户端发送证书、服务端检查
iii. 数据传输机密性：传输前客户端协商提出支持的非对称加密算法、摘要算法、对称加密算法、密钥长度等，服务端选择最安全的，结束协商（并开始互发证书，结束认证）客户端随机生成长字符串作为对称加密密钥，按服务端的公钥加密发送
iv. 防止重放攻击：使用加密的序列号作为数据包的负载，SSL握手中有随机数来标记，防止攻击者嗅探

3. Secure Electronic Transaction 安全电子交易 SET：VISA和Master Card两大信用卡公司联合推出的规范，在应用层解决用户商家银行间的信用卡交易

a. 提供的服务
    i. 通信管道、X.509v3证书、交易隐秘性
    ii. 机密性、数据完整性、身份认证、不可否认性
b. 参与者：持卡人cardholder、商店merchant、发卡银行issuer、收单银行acquirer、支付网关payment gateway、认证中心CA
c. 双重签名：让商店只处理order信息，银行只处理payment信息
    i. 先将两个信息的哈希摘要拼接，再哈希摘要、再用用户私钥加密
d. 交易阶段
    i. 购买请求阶段，持卡人与商家确定所用支付方式的细节
    ii. 支付的认定阶段，商家与银行核实，随着交易的进行，他们将得到支付
    iii. 收款阶段，商家向银行出示所有交易的细节，然后银行以适当方式转移货款
    iv. 在整个交易过程中，持卡人只和第一阶段有关，银行与第二、第三阶段有关，而商家与三个阶段都要发生联系。每个阶段都要使用不同的加密方法对数据加密，并进行数字签名。